IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	James Alexander Reeds III and Wen-Ping Ying		
Title:	APPARATUS, SYSTEM AND METHOD FOR VALIDATING INTEGRITY OF TRANSMITTED DATA		
Application No.:	09/879,575	Filed:	June 12, 2001
Examiner:	Ellen C. Tran	Group Art Unit:	2134
Atty. Docket No.:	037-0039	Confirmation No.:	4755

October 27, 2008

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed on July 30, 2008 and the Notice of Panel Decision from Pre-Appeal Brief Review, mailed August 15, 2008, setting a date for response of September 30, 2008. A petition for extension of time is being filed herewith (either as a separate paper or constructively in accordance with 37 C.F.R. § 1.136(a)(3)) thereby extending the period for reply until October 30, 2008.

Any fees required by this paper under 37 C.F.R. § 41.20(b)(2) are being provided as directed in an electronic submission of this paper or in a transmittal letter accompanying this paper. However, the Commissioner is hereby authorized to charge any deficiency in fees required by this paper and any additional fees under 35 C.F.R. § 1.16 or 1.17 which may be required during the pendency of this application, and to similarly credit any overpayment, to Deposit Account 50-0631.

REAL PARTY IN INTEREST

The real party in interest in this appeal is AT&T Mobility II LLC as evidenced by:

- Assignments from James Alexander Reeds III and Wen-Ping Ying to AT&T Wireless Services, Inc. and AT&T Corp. recorded in the Patent and Trademark Office at Reel 011906/Frame 0351; and

- An assignment from New Cingular Wireless Services, Inc. f/k/a AT&T Wireless Services, Inc. to Cingular Wireless II, Inc. recorded in the Patent and Trademark Office at Reel 017555/Frame 0711; and

- An assignment from Cingular Wireless II, Inc. to Cingular Wireless II, LLC recorded in the Patent and Trademark Office at Reel 017546/Frame 0612; and

- A Certificate of Conversion from Cingular Wireless II, Inc. to Cingular Wireless II, LLC recorded in the Patent and Trademark Office at Reel 017696/Frame 0375; and

- A Change of Name from Cingular Wireless II, LLC to AT&T Mobility II, LLC recorded in the Patent and Trademark Office at Reel 021290/Frame 0816; and

- A Change of Name from AT&T Mobility II, LLC to AT&T Mobility II LLC recorded in the Patent and Trademark Office at Reel 021313/Frame 0673.

RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision for this appeal.

STATUS OF CLAIMS

Claims 1-3, 5-16, 18-22, 26-32, 41-43, 45-47, and 57 are pending, stand as rejected, and are the subject of this appeal.

STATUS OF AMENDMENTS

An amendment subsequent to the final rejection was filed on June 9, 2008, and was entered for purposes of appeal as indicated by the Advisory action mailed June 20, 2008. The above-mentioned status of claims reflects the entry of this amendment.

SUMMARY OF CLAIMED SUBJECT MATTER

The independent claims involved in this appeal are claims 1, 14, 41, and 57. Independent claim 1 is directed to a method including selecting a fixed length segment of a continuous

decryption key stream based on a received session count of a received data packet. See e.g., steps 602, 604, 606, 608, and 622, see Fig. 6 and accompanying description, page 16, line 22-page 17, line 4 and page 17, line 29-page 18, line 6. The method includes padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size. See e.g., steps 622 and 624, see Fig. 6 and accompanying description, page 18, lines 7-10. The method includes decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload. See e.g., steps 622 and 626, see Fig. 6 and accompanying description, page 18, lines 11-16. A portion of the fixed length segment is applied to the encrypted payload and a remaining portion of the fixed length segment is applied to the padding. See e.g., step 626, see Fig. 6 and accompanying description, page 18, lines 11-16.

Independent claim 14 is directed to a method of generating an encrypted data packet including padding data to generate padded data. See e.g., steps 502, see Figs. 5a and 5b and accompanying description, page 14, lines 18-28, page 16, lines 1-17. The method includes selecting a fixed length segment of a continuous encryption key stream. See e.g., steps 518, see Fig. 5b and accompanying description, page 16, lines 5-10. The method includes applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding. See e.g., steps 518, see Fig. 5b and accompanying description, page 16, lines 5-10. The method includes de-padding the padded encrypted data to form the encrypted payload. See e.g., step 520, see Fig. 5b and accompanying description, page 16, lines 11-17. The method includes generating a session count based in accordance with the fixed length segment. See e.g., step 504, see Fig. 5a and accompanying description, page 14, lines 29-page 15, line 2. The method includes combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet. See e.g., step 512, see Fig. 5a and accompanying description, page 15, lines 17-26.

Independent claim 41 is directed to a transmitter configured to generate an encrypted data packet. See e.g., transmitter 106, Figs. 1 and 3 and accompanying description, page 6, lines 19-29. The transmitter includes a padding engine configured to generate padded data. See e.g., padding engine 326, see Fig. 3 and accompanying description, page 7, lines 1-14. The

transmitter includes an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data. See e.g., encryption engine 306, see Fig. 3 and accompanying description, page 7, lines 1-14. The transmitter includes a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload. See e.g., pad remover 328, see Fig. 3 and accompanying description, page 7, lines 1-14. The transmitter includes a session count generator configured to generate a packet number in accordance with the fixed length segment, the encrypted data packet comprising the encrypted payload and at least a portion of the session count. See e.g., session counter 324, see Fig. 3 and accompanying description, page 7, lines 1-14.

Independent claim 57 is directed to a receiver including a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold. See e.g., session count evaluator 418, see Fig. 4 and accompanying description, page 11, line 24-page 12, line 10. The receiver includes a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine. See e.g., padding engine 424, see Fig. 4 and accompanying description, page 12, lines 11-23. The receiver includes a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold. See e.g., decryption engine 406, see Fig. 4 and accompanying description, page 13, lines 8-27. The receiver includes a pad remover configured to remove padding from the decrypted data. See e.g., pad remover 428, see Fig. 4 and accompanying description, page 13, lines 17-19.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Ground I: The rejection of claims 1-3, 5-8, 14-16, 18-22, 26, 27, 41-43, and 45-47 under 35 U.S.C. § 103(a) as being unpatentable over U. S. Patent Application Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky") in view of U. S. Patent Application Publication No. 2001/0052072 to Jung (hereinafter, "Jung").

Ground II: The rejection of claims 9-13 and 28-32 under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of Jung, and further in view of U.S. Patent No. 6,105,012 to Chang et al. (hereinafter, "Chang").

Ground III: The rejection of claim 57 under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of U.S. Patent No. 6,918,034 to Sengodan et al. (hereinafter, "Sengodan").

ARGUMENT

In rejecting the claims, the Examiner engages in an examination that fails to establish a *prima facie* case of obviousness because the references fail to teach or suggest the claimed combination. See In re Nielson, 816 F.2d 1567, 1572, 2 USPQ2d (BNA) 1525, 1528 (Fed. Cir. 1987); see also In re Kahn, 441 F.3d 977, 986, 78 USPQ2d (BNA) 1329, 1335 (Fed. Cir. 2006).

In general, obviousness is a legal determination based on underlying factual inquiries. See Minnesota Min. & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc., 976 F.2d 1559, 1572-73, 24 USPQ2d (BNA) 1321, 1332-33 (Fed. Cir. 1992). Graham v. John Deere Co., 383 U.S. 1, 17 (1966) defines the factual inquiries utilized to evaluate the prior art. Specifically, the prior art is evaluated in terms of: (1) its scope and content; (2) the differences between the prior art and the claimed invention; (3) the level of ordinary skill in the art at the time the application was filed; and (4) objective, or secondary, evidence of nonobviousness such as commercial success, failure of others, long-felt need and unexpected results, which must be considered in reaching a conclusion of obviousness. See Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ (BNA) 459, 460 (1966); Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1566-67, 1 USPQ2d (BNA) 1593, 1595-96 (Fed. Cir. 1987); Minnesota Min. & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc., 976 F.2d 1559, 1573, 24 USPQ2d (BNA) 1321, 1333 (Fed. Cir. 1992).

In the present appeal, the issues relate to specific differences between the prior art and appealed claims. All claim limitations must be considered in the obviousness analysis. See Panduit Corp., 810 F.2d at 1576, 1 USPQ2d at 1603–04. None of the references, standing alone or in combination, teach or suggest all of the recited limitations.

Ground I: The rejection of claims 1-3, 5-8, 14-16, 18-22, 26, 27, 41-43, and 45-47 under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of Jung.

Claims 14-16, 18-22, 26, and 27

Specifically, regarding claim 14, Appellants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet,

as required by claim 14. Appellants respectfully point out that those limitations of the method of generating an encrypted data packet of claim 14 require both padding data and de-padding padded, encrypted data to form the encrypted payload.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference

> to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that decrypts incoming speech data packet and pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14. No other portion of Jung teaches those limitations of claim 14.

Appellants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Appellants maintain that the differences between the claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention). The Office has failed to establish that it is predictable to both pad data and de-pad padded, encrypted data to form the encrypted payload, as required by claim 14, based on padding data as taught by Jung. Appellants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 14. Therefore, independent claim 14 is allowable, as well as the claims depending therefrom. Accordingly, the PTO's rejection of claims 14-16, 18-22, 26, and 27, should be reversed.

Claims 41-43 and 45-47

Specifically, regarding claim 41, Appellants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> a padding engine configured to generate padded data,
> an encryption engine configured to apply a portion of
> a fixed length segment of a continuous encryption key

> stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload,

as required by claim 41. Appellants respectfully point out that those limitations of claim 41 require a transmitter that includes both a padding engine configured to generate padded data and a pad remover configured to generate the encrypted data packet.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, as required by claim 41.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that decrypts incoming speech data packet and pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest a padding engine configured to generate padded data, an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data, a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload, as required by claim 41. No other portion of Jung teaches those limitations of claim 41.

Appellants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Appellants maintain that the differences between the claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention).

The Office has failed to establish that it is predictable for a transmitter to include both a padding engine configured to generate padded data and a pad remover configured to generate the encrypted data packet, as required by claim 41, based on padding data as taught by Jung. Appellants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 41. Therefore, independent claim 41 is allowable, as well as the claims depending therefrom. Accordingly, the PTO's rejection of claims 41-43 and 45-47, should be reversed.

Claims 1-3 and 5-8

Specifically, regarding claim 1, Appellants respectfully maintain that Medvinsky, alone or in combination with Jung, fails to teach or suggest

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 1. Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to

> a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1.

Jung fails to compensate for the shortcomings of Medvinsky. Jung teaches that

> [t]he encryption/decryption module 24 is primarily responsible for encrypting the outgoing speech data packets and decrypting the incoming speech data packets. In one embodiment, a stream encryption algorithm is used by the encryption/decryption module 24 to encrypt and decrypt the data packets. Note, however, that the specific type of stream encryption algorithm used is not important to the invention, and that any known or yet to be developed stream encryption may be used without departing from the scope of the invention. The tasks performed by the encryption/decryption module 24 include such things as performing certain mathematical/logical operations on the data (depending on the type of encryption used), padding the data where applicable, and other tasks related to the encryption/decryption process.

Paragraph 0035 (emphasis added). The system of Jung includes an encryption/decryption module that decrypts incoming speech data packet and pads the data where applicable. Paragraph 0035. Padding data where applicable, as taught by Jung fails to teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload,

a remaining portion of the fixed length segment being applied to the padding, as required by claim 1. No other portion of Jung teaches those limitations of claim 1.

Appellants respectfully point out that in determining whether the subject matter of a patent claim is obvious, "[w]hat matters is the objective reach of the claim." KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 16; 82 USPQ2d 1385, 1397 (U.S. 2007). "If the claim extends to what is obvious, it is invalid under § 103." See id. To be nonobvious, an improvement must be "more than a predictable use of prior art elements according to their established functions." See id. at 13; 1396. Appellants maintain that the differences between the claim and the prior art are not predictable uses of prior art elements according to their established functions and the Office has failed to satisfy other obviousness inquiries (e.g., simple substitution of one known element for another to obtain predictable results, use of a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improvement to yield predictable results, known work in one field of endeavor prompting variations of it for use in the same field or a different one based on design incentives or other market forces if the variation would have been predictable to one of ordinary skill in the art, or some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the reference or to combine the prior art teachings to arrive at the claimed invention). The Office has failed to establish that it is predictable to pad an encrypted payload of a received data packet, as required by claim 1, based on padding data as taught by Jung. Appellants respectfully maintain that the Office's proposed combination is not a predictable use of the padding taught by Jung.

Thus, the combination of Medvinsky and Jung fails to establish a *prima facie* case of obviousness of the limitations of claim 1. Therefore, independent claim 1 is allowable, as well as the claims depending therefrom. Accordingly, the PTO's rejection of claims 1-3 and 5-8, should be reversed.

Ground II: The rejection of claims 9-13 and 28-32 under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of Jung, and further in view of U.S. Patent No. 6,105,012 to Chang et al. (hereinafter, "Chang").

Claims 28-32

Regarding claims 28-32, Appellants respectfully maintain that Medvinsky, alone or in combination with Jung and Chang, fails to teach or suggest

> padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet,

as required by claim 14 from which claims 28-32 indirectly depend. Appellants respectfully point out that those limitations of the method of generating an encrypted data packet of claim 14 require (and the references of record fail to teach or suggest) both padding data and de-padding padded, encrypted data to form the encrypted payload.

As described above with regard to the first ground of rejection, Medvinsky and Jung fail to teach or suggest those limitations of claim 14. Chang fails to compensate for the shortcomings of Medvinsky and Jung. Chang teaches a financial transaction processing system that transmits encrypted form data. Col. 2, lines 10-55. Chang teaches further that confidential information is encrypted with a session key that is attached to the encrypted data being sent to a client. Col. 9, lines 11-36. Nowhere does Chang teach or suggest padding data to generate padded data, applying the fixed length segment to the padded data to form padded encrypted data by applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding, de-padding the padded encrypted data to form the encrypted payload, and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet, as required by claim 14.

Since Medvinsky, Jung, and Chang fail to teach or suggest the limitations of claim 14 from which claims 28-32 indirectly depend, the PTO's rejection of claims 28-32 should be reversed.

Claims 9-13

Regarding claims 9-13, Appellants respectfully maintain that Medvinsky, alone or in combination with Jung and Chang, fails to teach or suggest

> padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 1 from which claims 9-13 indirectly depend. As described above with regard to the first ground of rejection, Medvinsky and Jung fail to teach or suggest those limitations of claim 1. Chang fails to compensate for the shortcomings of Medvinsky and Jung. Chang teaches a financial transaction processing system that transmits encrypted form data. Col. 2, lines 10-55. Chang teaches further that confidential information is encrypted with a session key that is attached to the encrypted data being sent to a client. Col. 9, lines 11-36. Nowhere does Chang teach or suggest padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 1.

Since Medvinsky, Jung, and Chang fail to teach or suggest the limitations of claim 1 from which claims 9-13 indirectly depend, the PTO's rejection of claims 9-13 should be reversed.

Ground III: The rejection of claim 57 under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of U.S. Patent No. 6,918,034 to Sengodan et al. (hereinafter, "Sengodan"). Appellants respectfully maintain that Medvinsky, alone or in combination with Sengodan, fails to teach or suggest

> a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data,

as required by claim 57. Appellants respectfully point out that those limitations of the receiver of claim 57 require (and the references of record fail to teach or suggest) both a padding engine and a pad remover.

Medvinsky teaches that

> [a]fter the encrypted data stream is received, processor 134 (of remote MTA 114) directs key stream generator 132 to output the same key stream bytes from the same key stream that was used to encrypt the voice packets at the local end. The key stream generator either generates the key stream bytes on-demand, or is free running based on the MTA clock and has the key stream bytes available by the time the RTP packet is received.
>
> Next, packet decryptor 130 XORs the key stream bytes with the encrypted data to recover the voice packets. The RTP time stamp is always incrementing to point to a unique place in the key stream such that packet decryptor 130 recovers the encrypted data. The present invention ensures that the key stream bytes are never repeated and thus enables secure communication of voice packets, even if a CODEC change or an SSRC collision occurs as further described with reference to FIG. 2. As used herein a "time stamp" is any mechanism for performing synchronization for a cipher in order to attain decryption of encrypted data.

Paragraphs 0033 and 0034 (emphasis added). The system of Medvinsky decrypts Real Time Protocol (RTP) packets by performing an XOR of received encrypted data packets with key stream bytes. Paragraph 0034. Nowhere does Medvinsky teach or suggest a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data, as required by claim 57.

Sengodan fails to compensate for the shortcomings of Medvinsky. Sengodan teaches that "[t]he recipient after decrypting the mini-packet looks at the last byte 524 to determine the number of padding bytes 522 used." Col. 8, lines 19-21. Even though Sengodan teaches a padding technique, that padding technique of Sengodan fails to teach or suggest a receiver that requires both a padding engine and a pad remover, as required by claim 57. Thus, Sengodan fails to teach or suggest a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine, a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, and a pad remover configured to remove padding from the decrypted data to recover the data, as required by claim 57.

Furthermore, Appellants respectfully point out that

> [o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate this review, this analysis should be made explicit.

KSR Int'l Co. v. Teleflex Inc., No. 04-1350, slip op. at 13; 82 USPQ2d 1385, 1396 (U.S. 2007). Moreover, "'[a] reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference or

would be led in a direction divergent from the path that was taken by the applicant.'" In re Kahn, 441 F.3d 977, 990, 78 U.S.P.Q.2d (BNA) 1329, 1338 (Fed. Cir. 2006) (citations omitted). The Office action fails to provide a proper rationale for combining Medvinsky with Sengodan to teach a receiver including both a padding engine and a pad remover, as required by claim 57. Sengodan teaches that "[b]lock encryption schemes require that the packet size be an integral multiple of block size." Col. 3, lines 54-55. Sengodan teaches that mini-packets are padded to "insure each mini-packet is an integral multiple of a predetermined block size." Col. 4, lines 34-36. "The padding added to the data for each packet comprises p-1 units of padding and a final padding unit for indicating the amount of padding" of Sengodan. Col. 4, lines 44-47. The final padding unit is transmitted with the padded mini-packet and received by a receiver of Sengodan. Col. 8, lines 9-21. The receiver of Sengodan that receives the encrypted padded data and an indicator of the amount of padding teaches away from a receiver including a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the padded encrypted payload of the received encrypted data received by the decryption engine, as required by claim 57.

Thus, the combination of Medvinsky and Sengodan fails to establish a *prima facie* case of obviousness of the limitations of claim 57. Accordingly, the PTO's rejection of claim 57 should be reversed.

CONCLUSION

For the at least the foregoing reasons, Appellants' presently claimed invention would not have been obvious to one of ordinary skill in the art under 35 U.S.C. § 103(a) in view of the cited prior art. Accordingly, this honorable Board is respectfully requested to reverse the rejections of claims 1-3, 5-16, 18-22, 26-32, 41-43, 45-47, and 57 and to direct the claims of the present application to be issued.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

/Nicole Teitler Cave/ — Nicole Teitler Cave

10/27/08 — Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

/Nicole Teitler Cave/

Nicole Teitler Cave, Reg. No. 54,021
Attorney for Applicant(s)
(512) 338-6315 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)

CLAIMS APPENDIX

1. A method comprising:

selecting a fixed length segment of a continuous decryption key stream based on a received session count of a received data packet; and

padding an encrypted payload of the received data packet to a given size with padding, the given size corresponding to the fixed length segment size, and

decrypting the payload of the received data packet by applying the fixed length segment of the continuous decryption key to the padded, encrypted payload, a portion of the fixed length segment being applied to the encrypted payload, a remaining portion of the fixed length segment being applied to the padding.

2. A method in accordance with claim 1, wherein the applying comprises performing a bit per bit stream decryption process.

3. A method in accordance with claim 2, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

5. A method in accordance with claim 2, further comprising:

receiving the data packet, the data packet comprising at least a portion of the received session count.

6. A method in accordance with claim 5, wherein the data packet further comprises at least a portion of a received message digest value.

7. A method in accordance with claim 5, wherein the selecting comprises:

selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

8. A method in accordance with claim 7, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

9. A method in accordance with claim 8, further comprising:

discarding the data packet if the difference is not less than the threshold value.

10. A method in accordance with claim 9, further comprising:

re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value.

11. A method in accordance with claim 6, further comprising:

discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value.

12. A method in accordance with claim 11, further comprising:

re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

13. A method in accordance with claim 12, further comprising:

extracting the at least a portion of the received message digest value from the data packet;

generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form a truncated message digest; and

comparing the truncated message digest to the at least a portion of the received message digest value.

14. A method of generating an encrypted data packet, the method comprising:
padding data to generate padded data;
selecting a fixed length segment of a continuous encryption key stream;
applying the fixed length segment to the padded data to form padded encrypted data by
applying a portion of the fixed length segment to the data to form an encrypted payload and applying a remaining portion of the fixed length segment to the padding;
de-padding the padded encrypted data to form the encrypted payload;
generating a session count based in accordance with the fixed length segment; and
combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet.

15. A method in accordance with claim 14, wherein the applying comprises performing a bit per bit streaming encryption process.

16. A method in accordance with claim 15, wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet.

18. A method in accordance with claim 14, further comprising:
generating a message digest value; and
combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet.

19. A method in accordance with claim 18, wherein the generating comprises:
generating the message digest value based on the encrypted payload, the session count and a message digest key.

20. A method in accordance with claim 18, further comprising:
forming the at least a portion of the message digest value by truncating the message digest value.

21. A method in accordance with claim 14, further comprising transmitting the encrypted data packet to a receiver through a communication channel.

22. A method in accordance with claim 14, further comprising:

receiving a received data packet corresponding to the encrypted data packet,

the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value;

selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and

decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet.

26. A method in accordance with claim 22, wherein the selecting the fixed length segment of the continuous decryption key stream comprises:

selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value.

27. A method in accordance with claim 26, wherein the selecting further comprises:

extracting the at least a portion of the received session count from the received encrypted data packet;

expanding the at least a portion of the received session count to the received session count; and

comparing the received session count to the locally generated session count.

28. A method in accordance with claim 27, further comprising:

discarding the received encrypted data packet if the difference is not less than the threshold value.

29. A method in accordance with claim 28, further comprising:

re-synchronizing the decryption key to the encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value.

30. A method in accordance with claim 26, further comprising:

discarding the received encrypted data packet if the received truncated message digest value does not match a truncated locally generated message digest value.

31. A method in accordance with claim 30, further comprising:

re-synchronizing the decryption key stream to an encryption key stream by setting the decryption key stream and the encryption key stream to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value.

32. A method in accordance with claim 31, further comprising:

extracting the received truncated message digest value from the received encrypted data packet;

generating a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key;

truncating the locally generated message digest value to form the locally generated truncated message digest value; and

comparing the locally generated truncated message digest value to the received truncated message digest value.

41. A transmitter configured to generate an encrypted data packet, the transmitter comprising:

a padding engine configured to generate padded data;

an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to the padded data to form encrypted padded data;

a pad remover coupled to receive the encrypted padded data from the encryption engine and operable to remove the encrypted padding to generate an encrypted payload; and

a session count generator configured to generate a packet number in accordance with the fixed length segment, the encrypted data packet comprising the encrypted payload and at least a portion of the session count.

42. A transmitter in accordance with claim 41, wherein the encryption engine is configured to perform a bit per bit streaming encryption process.

43. A transmitter in accordance with claim 42, wherein the encryption engine is further configured to perform an exclusive OR operation with the portion of the fixed length segment and the data packet.

45. A transmitter in accordance with claim 42, further comprising:

a message digest generator configured to generate a message digest value, the encrypted data packet comprising at least a portion of the message digest value.

46. A transmitter in accordance with claim 45, wherein the message digest generator is further configured to generate the message digest value based on the encrypted payload, the session count and a message digest key.

47. A transmitter in accordance with claim 46, further comprising:

a truncator configured to truncate the message digest value to form the at least a portion of the message digest value.

57. A receiver comprising:

a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold;

a padding engine operable to pad an encrypted payload of the received encrypted data packet to generate the payload of the received encrypted data received by the decryption engine;

a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous

decryption key stream to the data packet if the difference is less than the threshold; and

a pad remover configured to remove padding from the decrypted data.

EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. § 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellants in the appeal.

RELATED APPEALS APPENDIX

There are no decisions rendered by a court or the Board in any proceeding identified above in the Related Appeals and Interferences section.